Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 4, Issue 5; October-December, 2017, pp. 332-333
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

Cyber Security for Digital Payment

Mayank Jain[1] and Aquil Ahmad Khan[2]

[1,2]ICERT, New Delhi
E-mail: [1]engineermayankjain@gmail.com,[2]akhan2786@gmail.com

Abstract—*The rise of new business models which depend on electronic payment systems, making another threat and vulnerability which prompts risk. In last decade, the number of malicious applications was developed to target online banking transactions. Therefore, there is a challenge not only to the users but also on digital payment systems. This paper will focus on the as assessment and analysis of threat and vulnerabilities within the context of a digital payment.*

Keywords: *Digital payment, vulnerabilities.*

1. INTRODUCTION

The technology used in digital payment are electronic for delivery of banking services and products. digital payment system has broken all the barriers of conventional branch banking. It eliminate the gap of customer understanding of the banking transactions and their participation in improving the sophistication of these services.

2. TYPES OF ATTACKS ON DIGITAL PAYMENT

Attackers usually exploit known Vulnerabilities in particular operating systems. They also may try repeatedly to make an unauthorized entry into a Web site during a short time frame thus denying service to other customers.

Phishing

An e-mail come from a legitimate organization such as a bank or E-commerce requests the user to update or to verify his/her personal and financial information which includes credit card numbers, date of birth, login credentials, account details and PINs etc. The e-mail usually contains a link that takes him/her to a spoof website that looks identical to the organization's genuine site. The attacker can then capture personal data such as passwords and other financial details.

Pharming

Pharming is similar to phishing. Attacker creates false websites and attacker redirect traffic from a genuine website to their own. The 'pharmer' or attacker will then try to obtain PINs, Passwords, Credit card numbers etc when user enter them into the false website.

Voice-over-IP

VoIP (voice over IP) is used to manage the delivery of voice information over the Internet. Voice over IP involves Sending voice information in digital form in discrete packets. A real person and caller ID is easily spoofed by an attacker.

Man-in-the-middle attacks

This type of attack happens when an attackers involve between two parties communicating with each other. VoIP is best example of man-in-the-middle attacks. the attacker intercepts Session Initiation Protocol (SIP) message traffic and masquerades as the called party to the calling party, or vice versa. attacker can hijack calls via a redirection server.

Malware attacks

A malicious software includes viruses, worms, Trojan horses and spyware is malware. Attackers try to send the malware through attachments. Panda Banker, Dark Pulsar, Kuik Adware, Emotet Trojan, are latest malware with advanced features like file exfiltration, remote command execution.

Automated Reply

Nowadays banks uses the automated answering system. Combined with war-dialling techniques and VoIP, an attacker can steal details like credit card numbers and user credentials.

Trojan horse

A programmer can embed code into a system to allow the unauthorized entrance into the network.

Sniffers

Sniffer or network monitors software used to capture keystrokes and login ID's and passwords.

Brute force

It is a trial and error method to decode encrypted data such as user credentials, Data Encryption Standard keys, through brute force.

Social Engineering

An attacker impersonating an authorized user to gain information about the system including changing passwords.

Hijacking

Intercepting transmissions then attempting to deduce information from them. Internet traffic is particularly vulnerable to this threat.

3. MITIGATION MEASURES

The banks ensure that transactions made through digital payment channel are safe and secure. Electronic payment systems becoming vulnerable to new types of misuse. The authentication measures of the customers should be more secure, Acritical approach to online banking fraud monitoring that analyzes the login event, the outgoing transaction and risky sequences of events to minimize online banking fraud.

During Login events of a user IP address and session ID profiling must be monitor. Also users Navigation events, Payee events, Profile events, Password events must be critically monitor by proper monitoring intelligence agency can get strong patterns of criminal intent. Active content monitoring and filtering can examine potentially destructive content material entering a network. virus scanners that scans and cleans networks must be periodically updated.

Intrusion Detection Systems

Network intrusion detection systems monitor network traffic and alert when someone is attempting to gain unauthorized access.

Firewall

A firewall is a system that implements the access-control policy between two networks. A firewall is a network security system that controls incoming and outgoing network traffic based on a set of rules. Firewall is a virtual security guard that protect a network’s integrity.

Penetration Testing

Penetration testing companies simulate attacks on networks to test for a system’s inherent weaknesses. Vulnerability-based scanning tools provide a snapshot of a system’s vulnerabilities.

Cryptographic Communications

Encryption uses complex algorithms to shield messages transmitted over channels. It provides safe passage to data transmission from source to destination. At the destination the message is decrypted using another algorithm.

4. CONCLUSION

The security models presently used in digital payment systems are based on user identification and authentication methods. Currently the attacks target the digital payment systems to the user focusing on obtaining authentication and identification information through the use of social engineering Banks should provide security mechanism which should be as user independent as possible. Mitigating the risk of user related information’s leaks and security issues affecting the system and leads to fraud.

REFERENCES

[1] Kulkarni, P G (1997). "Trends and Effectiveness of IT in Banking Sector," in Kanungo, Shivraj (ed.), Information Technology at Work—A Collection of Managerial Experiences, New Delhi: Hindustan Publishing Corporation

[2] Threats to online Banking published by virus bulletin, July 2005

[3] www.ijaiem.org/volume2Issue3/IJAIEM-2013-03-15

[4] Lucas, H C (1994). Information Systems Concepts for Management,San Francisco: McGraw-Hill.

[5] HALLER, N. A One-Time Password System (RFC 2289). Internet Engineering Task Force. [S.l.].1998

[6] CAVUSOGLU, Hasan e Cavusoglu, Huseyin. Emerging Issues in Responsible Vulnerability Disclosure. Workshop on Information Technology and Systems (WITS 2004). Barcelona, Spain, 2004.

[7] O. Dandash, P. Dung Le, and B. Srinivasan, Internet banking payment protocol with fraud prevention, 2007

[8] www.researchmanuscripts.com/isociety2012/6